Enterprise Information Services
Duty Statement

Section:	Information Security Office
Unit:	Information Security Office
Position Number:	065-644-1312-001
Classification:	Staff Information Systems Analyst (Specialist)
Date:	March 2015

Supervision: Under the general supervision of the Data Processing Manager IV, the Staff Information Systems Analyst (Specialist) is responsible for the maintenance of the department's eDiscovery program. The incumbent receives assignments in terms of broadly defined missions or functions, and operates within a largely unsupervised environment, but within a clear accountability framework.

The Staff Information System Analyst (Specialist) is required to fulfill eDiscovery requests, create and publish related policies and standards, implement and administer archiving and searching platforms, and works closely with the legal department's resources to provide necessary evidence and litigation support. Strong knowledge of email systems, network file storage, databases, and other common data repositories is required. Knowledge regarding data retention policy and practice is required. The highest degree of confidentiality and integrity while handling eDiscovery matters is expected.

Additionally, the incumbent is responsible for supporting the Disaster Recovery Planning effort, the Risk Assessment Program, and acts as a liaison for the Information Security Office (ISO) and CDCR organizational units. Duties will include planning, designing, and carrying out programs, studies or other work with little direction from the supervisor.

Incumbents at the staff level will either take responsibility for substantial technical decision-making or for teams of staff and supporting information technology application components. As such, the incumbent must be able to demonstrate the basic competencies associated with team leadership with a high degree of technical versatility and broad industry knowledge.

Knowledge: This is the journey level. It is expected that the incumbent will demonstrate true proficiency with respect to data processing concepts, practices, methods, and principles along with an understanding of and currency with respect to evolving industry trends and standards. Incumbents demonstrate the ability to effectively apply this knowledge in evaluating alternative proposals and recommending optimal solutions, including:

- Experience in operating eDiscovery processing tools and platforms.
- Experience with both keyword and concept-based search methodologies.
- Basic understanding of data encryption/decryption technologies and tools.
- Proficiency in administering Windows Servers.
- Extensive knowledge of the available tools, methods and procedures associated with the protection of information assets. The incumbent is experienced in enterprise system data security, data backup and data recovery.
- Ability to apply concepts such as portability and scalability in evaluating long term, complex information technology systems.
- Ability to take into account the larger business perspective in proposing and designing information security solutions.
- Knowledge of the roles and responsibilities of oversight and regulatory agencies in assuring security and compliance.

- Ability to work independently in effectively securing resources and expertise through proper channels within the organization, while developing and managing large and complex systems.
- Extensive knowledge of the business enterprise, including goals and mission of the organization.

Guidelines: Administrative and technical policies and precedents are applicable, but are stated in general terms. The incumbent is thoroughly familiar with the available tools, methods, and procedures with eDiscovery and in the ISO and the EIS. The incumbent uses initiative and resourcefulness in deviating from traditional methods or in researching emerging technologies to develop new methods, criteria, and/or new policies. The incumbent uses judgment in interpreting and adapting guidelines such as policies, operations manuals, and work directions for application to specific cases or problems. The incumbent is also able to apply selected technical tools, guidelines, etc., in such a way as to meet set targets of cost, time, quality, and performance.

Complexity: The work includes varied duties requiring many different and unrelated processes and methods applied to a broad range of activities or substantial depth of analysis. The work requires originating new techniques, establishing criteria, or developing new information. The work also involves demonstrating leadership in identifying new issues and business opportunities and in assisting management with the most sensitive issues. Incumbents demonstrate an in-depth understanding of the relationship of their technical specialization and/or project responsibilities to the work as a whole. Incumbents are able to propose technical solutions within their scope of expertise which take into account the customer's business needs. Presentations will typically be a routine function of the job. Incumbents must demonstrate an in-depth understanding of the relationship of their technical role with respect to the overall EIS function and the various business groups.

Scope and Effect: Full competence in a specialized analytical role is demonstrated at this level of proficiency. Technical accountability for work done and decisions taken is expected. The ability to give technical or team leadership is demonstrated at this level with a high degree of technical versatility and broad industry knowledge. The scope of the work involves isolating and defining unknown conditions, using technologies to resolve critical problems, and developing new applications of existing technologies. The work product or service affects the work of other experts, the development of major aspects of technology projects, programs or missions, or the products and services of substantial numbers of people. This is the work of a clearly defined specialist. On a regular basis, incumbent is expected to complete assignments involving multiple tasks, single significant functions, or multiple functions. Because of the mission-criticality of the EIS systems, the incumbent's work products affect the security of all CDCR systems.

Personal Contact: The incumbent contacts managers, technical staff, and systems users to provide and make recommendations regarding systems and problems requiring solutions. There is regular contact with IT staff, vendors, and external entities to coordinate problem solving and ensure conformity of methods and practices. The incumbent contacts users to discuss security requirements, contractors to provide oversight, and vendors to discuss existing or new technology. Incumbents communicate effectively, both orally and in writing with subordinates, peers, clients, and customers at all levels. The incumbent demonstrates proficiency in presentations on product deliverables, and has the ability to influence, motivate, persuade, and lead individuals or groups. The incumbent must develop knowledge of the roles and

responsibilities of the state's oversight and regulatory agencies, since proposals will be presented to these entities for approval. The incumbent possesses the necessary general and technical competencies to prioritize work, initiate contacts, and resolve issues. In order to be successful, the incumbent is expected to develop a solid understanding of the various business functions of the different CDCR organizations.

Purpose of Contacts: The incumbent influences, motivates, persuades, and leads individuals or groups. Those contacted may be hesitant or skeptical, so the incumbent must be skillful in approaching the individual or group in order to obtain the desired response (i.e., obtain agreement where there is controversy and dissimilar goals).

The actual duties of the incumbent include the following:

60%	eDiscovery

- Conduct searches and provide technical support for requests from CDCR's Office of Legal Affairs or the California Deputy Attorney General's office for email, instant messaging in support of regulatory or litigation.
- Translate business requirements for document recovery into search terms that can be used by journaling and archiving systems.
- Ensure archiving solutions support the department's retention policies.
- Process litigation hold requests.

15%	Disaster Recovery Planning

- Participate as a team member to develop, implement, and maintain the Technical Recovery Plan (TRP).
- Assist with gathering the TRP documents from all local institutions and organizational units.
- Implement the TRP template established by the State ISO and provide support in the form of reviewing and selection of testing scenarios for local TRP coordinators.
- Review and coordinate the annual submission of the California Department of Corrections and Rehabilitation (CDCR) TRP to the Office of the Chief Information Officer, State Information Security Office.

10%	Risk Assessment Program Coordination

- Coordinate and facilitate mitigation efforts identified in or recommended as a result of the Risk Assessment reviews conducted as part of the Risk Assessment Management Program (RAMP).
- Interface with CDCR organizational units to make operational improvements through training, consensus, and cooperation.

10%	Information Security Liaison

- Serve as an information source to staff requiring guidance in resolution of complex technical and analytical problems involving disaster recovery.
- Attend monthly field staff meetings to enhance user awareness and training on their role in the event of a loss of service.
- Review and provide input to project initiation documents such as Feasibility Study Reports, Special Project Reports, Project Summary Packages and budget documents to verify that operation recovery processes are included.

5%	**Policies, Standards, Training and Others**

- Provide backup to the CDCR Information Security Officer and the Information Security Office staff for related Risk Assessment functions.
- Attend training, seminars, and conferences, as required.
- Expected to communicate effectively both orally and in writing with subordinates, peers, clients, and customers at all levels.
- Participate in hardware and software procurements.
- Participate in EIS and ISO unit meetings and other activities as required.

Employee: _____ Date: _____

Immediate Supervisor: _____ Date: _____